Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-2 and 4-56 are pending in the application, with claims 1, 11, 20, 24, 31 and 40 being the independent claims. Claims 1, 8, 10, 11, 15, 17, 20, 24-41, 45-47 and 49 are sought to be amended. Claims 51-56 are sought to be added. Claim 3 is sought to be cancelled without prejudice or disclaimer of the subject matter therein. Applicants reserve the right to prosecute similar or broader claims, with respect to the amended claims, in the future. These changes and additions introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-10, 24-31, 33-42, and 45-50 under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 7,046,807 to Hirano *et al.* ("Hirano"). Applicants respectfully traverse this rejection. In addition, some clarifying amendments are made.

Claims 1-10

The Examiner contends that Hirano teaches each of the elements of independent claim 1, Applicants respectfully disagree. Claim 1, as amended, recites a computer implemented method for securing a file in an application environment, the method comprising:

> ***determining, in an operating system*** supporting an application, whether the file being accessed is secured when a request to access the file is received;
>
> if the file is determined to be secured, activating a cipher module and loading the file through the cipher module into the application; and
>
> if the file is determined to be non-secured, loading the file into the application without activating the cipher module;
>
> ***wherein the cipher module, once activated, operates transparently to a user requesting an access to the file***

Applicants maintain that Hirano does not teach or suggest each and every feature of claim 1, as amended. For example, Hirano does not teach or suggest "*determining, in an operating system supporting an application, whether the file being accessed is secured when a request to access the file is received; if the file is determined to be secured, activating a cipher module and loading the file through the cipher module into the application; wherein the cipher module, once activated, operates transparently to a user requesting an access to the file,*" as recited in claim 1, as amended.

First, the Examiner, on pages 2 and 3 of the Office Action, appears to rely upon column 5, lines 3-23 and column 7, line 55 through column 8, line 2 of Hirano to allegedly show the features of "*determining, in an operating system supporting an application, whether the file being accessed is secured when a request to access the file is received; if the file is determined to be secured, activating a cipher module and loading the file through the cipher module into the application*" as recited in claim 1. Applicants respectfully disagree.

Hirano is directed to a data administration method which prevents the infringement of a copyright by encrypting and distributing digital content. In the method of Hirano, synthetic data (Hirano Fig. 1, element 12) includes a real data section (Hirano

Fig. 1, element 15) which is *encrypted digital content*, a header data section (Hirano Fig. 1, element 16) which includes *consent information*. The c*onsent information* contains information of a contents key that is used as an encryption key to encrypt the digital content (Hirano Col. 5, Lines 4-19). The *consent information* is *encrypted* by an encryption key based on *user information* and can be decoded using the user information (Hirano Col. 10, Lines 12-14). Moreover, *privileges information* including the copyright information of the digital content is embedded in the digital content. Further, on the contents user side, there are user information managing section, synthetic data obtaining section, header data display section, consent information extracting section, a contents key decrypting section, a contents decrypting section, and a *contents operating section* (Hirano Col. 7, Line 55 to Col. 8 Line 2). But no where in Hirano (including the sections cited by the Examiner) it is taught or suggested that it is determined in an operating system supporting an application whether the file being access is secured, as recited in claim 1.

Second, Applicants maintain that Hirano does not teach or suggest the feature of "*wherein the cipher module, once activated, operates transparently to a user requesting an access to the file,*" as recited in claim 1, as amended. In contrast, "content user 3 transmits the user information 14 to the contents manager 2 in the case where the contents user 3 would like to employ the digital content that the contents manager 2 manages" (Hirano Col. 6, Lines 34-37). Hirano discloses a method wherein each time the user needs to utilize the digital content, the user has to transmits its information to the contents manager. Contrast this to the claim 1 cipher module which once activated, ***operates transparently to a user*** requesting an access to the file, as recited in claim 1.

For at least the reasons set forth above, Applicants submit that independent claim 1 is patentable over Hirano.

Furthermore, claims 2-10, all of which depend from and further limit independent claim 1, are also patentable over Hirano for the same reasons set forth above with respect to independent claim 1, and further in view of their own respective features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection, and find claims 1-10 allowable over the applied reference.

Claims 24-30

The Examiner contends that Hirano teaches each of the elements of independent claim 24, Applicants respectfully disagree. Claim 24, as amended, recites a computer readable storage medium having computer program code recorded thereon, that when executed by a processor, causes the processor to access a file in an application environment by a method, comprising:

> ***determining, in an operating system***, whether the file being accessed is secured when a request to access the file by an application is received;
> if the file is determined to be secured,
> ***activating a cipher module that operates in the operating system***;
> loading the file through the cipher module into the application;
> if the file is determined to be non-secured,
> loading the file into the application without activating the cipher module;
> ***wherein the cipher module, once activated, operates transparently to a user requesting an access to the file.***

Applicants maintain that Hirano does not teach or suggest each and every feature of claim 24, as amended. For example, for the reasons set forth above with respect to claim 1, Hirano does not teach or suggest "*determining, in an operating system, whether*

the file being accessed is secured when a request to access the file by an application is received; if the file is determined to be secured, activating a cipher module that operates in the operating system; loading the file through the cipher module into the application; wherein the cipher module, once activated, operates transparently to a user requesting an access to the file," as recited in claim 24, as amended.

For at least the reasons set forth above, Applicants submit that independent claim 24 is patentable over Hirano.

Furthermore, claims 25-30, all of which depend from and further limit independent claim 24, are also patentable over Hirano for the same reasons similar to those set forth above with respect to independent claim 24, and further in view of their own respective features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection, and find claims 24-30 allowable over the applied reference.

Claims 31 and 33-39

The Examiner contends that Hirano teaches each of the elements of independent claim 31, Applicants respectfully disagree. Claim 31 recites a computer readable storage medium having computer program code recorded thereon, that when executed by a processor, causes the processor to secure a file in an application environment by a method, comprising:

> ***maintaining a file key in a temporary memory space;***
>
> encrypting the file with the file key in a cipher module to produce an encrypted file, wherein the file has been opened with an application and the ***cipher module operates transparently as far as a user executing the application is concerned;*** and

> storing, in a storage space, a secured file including the encrypted file and a header, wherein the header includes or points to security information including the file key.

Applicants maintain that Hirano does not teach or suggest each and every feature of claim 31. For example, Hirano does not teach or suggest *"maintaining a file key in a temporary memory space; encrypting the file with the file key in a cipher module to produce an encrypted file, wherein the file has been opened with an application and the cipher module operates transparently as far as a user executing the application is concerned,"* as recited in claim 31.

First, it is noted that no where in Hirano it is taught or suggested that a file key is maintained in a temporary memory spaces, as recited in claim 31. The Examiner, on page 8 of the Office Action, with regard to claim 11 states:

> The teachings of Hirano et al fail to disclose of maintaining a file key in a temporary memory space. It is taught by Novak of maintaining a file key in a temporary memory space (col. 12, lines 16-28). (Office Action, Page 8, Lines 6-9)

This was the reason that the Examiner introduced the new reference Novak (U.S. Patent No. 7,046,807) to allegedly reject claim 11.

Second, Hirano does not teach or suggest that the cipher module operates transparently as far as a user executing the application is concerned, as recited in claim 31. In contrast, "content user 3 transmits the user information 14 to the contents manager 2 in the case where the contents user 3 would like to employ the digital content that the contents manager 2 manages" (Hirano Col. 6, Lines 34-37). Therefore, Hirano discloses a method wherein each time that the user needs to utilize the digital content, the user has to transmits its information to the contents manager. This is in contrast to the cipher

module of claim 31 that ***operates transparently as far as user*** is concerned, as recited in claim 31.

For at least the reasons set forth above, Applicants submit that independent claim 31 is patentable over Hirano.

Furthermore, claims 33-39, all of which depend from and further limit independent claim 31, are also patentable over Hirano for the same reasons similar to those set forth above with respect to independent claim 31, and further in view of their own respective features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection, and find claims 31 and 33-39 allowable over the applied reference.

Claims 40-42 and 45-50

The Examiner contends that Hirano teaches each of the elements of independent claim 40, Applicants respectfully disagree. Claim 40 recites a computing device for securing a file in an application environment, the computing device comprising:

> an application, when executed, accessing the file that includes security information and an encrypted portion, the ***security information*** further including ***a file key*** and ***access rules***, and the encrypted portion being an encrypted version of the file;
>
> a cipher module activating upon determining that the file being accessed is secured;
>
> wherein the ***security information is encrypted with a user key*** and can be decrypted with the user key when authenticated; and
>
> wherein the file key can be retrieved to decrypt the encrypted portion only after the access rules have been successfully measured against access privilege of the user.

Applicants maintain that Hirano does not teach or suggest each and every feature of claim 40. For example, Hirano does not teach or suggest "*an application, when executed, accessing the file that includes security information and an encrypted portion, the security information further including a file key and access rules, and the encrypted portion being an encrypted version of the file; wherein the security information is encrypted with a user key and can be decrypted with the user key when authenticated*," as recited in claim 40. In contrast, in the method of Hirano, privileges information is embedded in digital content and the digital content is encrypted using a contents key and the content key is encrypted using user information.

Hirano is directed to a data administration method which prevents the infringement of a copyright by encrypting and distributing digital content. In the method of Hirano, synthetic data (Hirano Fig. 1, element 12) includes a real data section (Hirano Fig. 1, element 15) which is *encrypted digital content*, a header data section (Hirano Fig. 1, element 16) which includes *consent information*. The *consent information* contains information of a contents key that is used as an encryption key to encrypt the digital content (Hirano Col. 5, Lines 4-19). The *consent information* is *encrypted* by an encryption key based on *user information* and can be decoded using the user information (Hirano Col. 10, Lines 12-14). Moreover, *privileges information* including the copyright information of the digital content is embedded in the digital content.

First, it is noted that the privileges information of Hirano is not the same as the access rules as recited in claim 40. The privileges information exhibits the copyright information and the publish privileges information of the digital content (Hirano Col. 8, Lines 39-43) which is not the same as the access rules of claim 40.

Second, in the method of Hirano, the privileges information is embedded in the digital content which is encrypted using a contents key. Further, the information of a contents key which is included in the consent information is encrypted by an encryption key based on user information. In contrast, claim 40 recites that security information that includes access rules and a file key is encrypted with a user key and the file is encrypted with the file key.

For at least the reasons set forth above, Applicants submit that independent claim 40 is patentable over Hirano.

Furthermore, claims 41-42 and 45-50, all of which depend from and further limit independent claim 40, are also patentable over Hirano for the same reasons similar to those set forth above with respect to independent claim 40, and further in view of their own respective features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection, and find claims 40-42 and 45-50 allowable over the applied reference.

Rejections under 35 U.S.C. § 103

The Examiner rejected claims 11-23, 32, 43, and 44 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hirano in view of U.S. Patent No. 6,865,555 to Novak ("Novak"). Applicants respectfully traverse this rejection.

Claims 11-19

The Examiner contends that the combination of Hirano and Novak teaches each of the elements of independent claim 11, Applicants respectfully disagree. Claim 11 recites a computer implemented method for securing a file in an application environment, the method comprising:

> maintaining a file key in a temporary memory space;
> encrypting the file with the file key in a cipher module to produce an encrypted portion;
> preparing security information for the encrypted portion, the ***security information being encrypted with a user key*** and ***including the file key and access rules*** to control access to the encrypted portion; and
> attaching the encrypted security information to the encrypted portion.

Applicants maintain that the combination of Hirano and Novak does not teach or suggest each and every feature of claim 11. For example, the combination of Hirano and Novak does not teach or suggest "*preparing security information for the encrypted portion, the security information being encrypted with a user key and including the file key and access rules to control access to the encrypted portion*," as recited in claim 11, as amended. In contrast, in the method of Hirano, privileges information is embedded in digital content and the digital content is encrypted using a contents key and the content key is encrypted using user information.

Hirano is directed to a data administration method which prevents the infringement of a copyright by encrypting and distributing digital content. In the method of Hirano, synthetic data (Hirano Fig. 1, element 12) includes a real data section (Hirano Fig. 1, element 15) which is *encrypted digital content*, a header data section (Hirano Fig. 1, element 16) which includes *consent information*. The *consent information* contains

information of a contents key that is used as an encryption key to encrypt the digital content (Hirano Col. 5, Lines 4-19). The *consent information* is *encrypted* by an encryption key based on *user information* and can be decoded using the user information (Hirano Col. 10, Lines 12-14). Moreover, *privileges information* including the copyright information of the digital content is embedded in the digital content.

First, it is noted that the privileges information of Hirano is not the same as the access rules as recited in claim 11. The privileges information exhibits the copyright information and the publish privileges information of the digital content (Hirano Col. 8, Lines 39-43) which is not the same as the access rules of claim 11 that controls access to an encrypted portion of a file.

Second, in the method of Hirano, the privileges information is embedded in the digital content which is encrypted using a contents key. Further, the information of a contents key which is included in the consent information is encrypted by an encryption key based on user information. In contrast, claim 11 recites that security information that includes access rules and a file key is encrypted with a user key and the file is encrypted with the file key.

Further, Novak fails to cure the deficiencies of Hirano as noted above. Novak does not teach what is missing from Hirano, for example security information being encrypted with a user key and including the file key and access rules to control access to the encrypted portion which is disclosed in claim 11. Therefore, for at least the reasons set forth above, Applicants submit that independent claim 11 is patentable over Hirano and Novak taken alone or in combination.

Furthermore, claims 12-19, all of which depend from independent claim 11, are also patentable over the combination of Hirano and Novak for reasons similar to those set forth above with respect to independent claim 11, and further in view of their own respective features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection, and find claims 11-19 allowable over the applied references.

Claims 20-23

The Examiner contends that the combination of Hirano and Novak teaches each of the elements of independent claim 20, Applicants respectfully disagree. Claim 20 recites a computer implemented method for providing access control to a file in an application environment, the method comprising:

> forwarding a request to access the file to a file system manager in an operating system;
> activating a document securing module by the file system manager to determine whether the file being accessed is secured;
> activating a cipher module when the file is determined to be secured; and
> loading the file through the cipher module into an application;
> ***wherein the cipher module, once activated, operates transparently to a user requesting an access to the file***

Applicants maintain that the combination of Hirano and Novak does not teach or suggest each and every feature of claim 20. For example, the combination of Hirano and Novak does not teach or suggest "*activating a document securing module by the file system manager to determine whether the file being accessed is secured; wherein the cipher module, once activated, operates transparently to a user requesting an access to the file,*" as recited in claim 20, as amended.

First, the Examiner, on page 10 of the Office Action, appears to rely upon column 7, line 55 through column 8, line 2 of Hirano to allegedly show the features of "*activating a document securing module by the file system manager to determine whether the file being accessed is secured*" as recited in claim 20. Applicants respectfully disagree.

Hirano is directed to a data administration method which prevents the infringement of a copyright by encrypting and distributing digital content. In the method of Hirano, synthetic data (Hirano Fig. 1, element 12) includes a real data section (Hirano Fig. 1, element 15) which is *encrypted digital content*, a header data section (Hirano Fig. 1, element 16) which includes *consent information*. The c*onsent information* contains information of a contents key that is used as an encryption key to encrypt the digital content (Hirano Col. 5, Lines 4-19). The *consent information* is *encrypted* by an encryption key based on *user information* and can be decoded using the user information (Hirano Col. 10, Lines 12-14). Moreover, *privileges information* including the copyright information of the digital content is embedded in the digital content. Further, on the contents user side, there are user information managing section, synthetic data obtaining section, header data display section, consent information extracting section, a contents key decrypting section, a contents decrypting section, and a *contents operating section* (Hirano Col. 7, Line 55 to Col. 8 Line 2). But no where in the sections of Hirano recited by the Examiner and no where in Hirano it is taught or suggested activating a document securing module by the file system manager to determine whether the file being accessed is secured, as recited in claim 20.

Second, Applicants maintain that Hirano does not teach or suggest the feature of "*wherein the cipher module, once activated, operates transparently to a user requesting an access to the file,*" as recited in claim 20, as amended. In contrast, "content user 3 transmits the user information 14 to the contents manager 2 in the case where the contents user 3 would like to employ the digital content that the contents manager 2 manages" (Hirano Col. 6, Lines 34-37). Therefore, Hirano discloses a method wherein each time that the user needs to utilize the digital content, the user has to transmits its information to the contents manager. This is in contrast to the cipher module of claim 20 which once activated, ***operates transparently to a user*** requesting an access to the file, as recited in claim 20.

Further, Novak fails to cure the deficiencies of Hirano as noted above. Novak does not teach what is missing from Hirano, for example activating a document securing module by the file system manager to determine whether the file being accessed is secured; wherein the cipher module, once activated, operates transparently to a user requesting an access to the file which is disclosed in claim 20. Therefore, for at least the reasons set forth above, Applicants submit that independent claim 20 is patentable over Hirano and Novak taken alone or in combination.

Therefore, for at least the reasons set forth above, Applicants submit that independent claim 20 is patentable over the combination of Hirano and Novak.

Furthermore, claims 21-23, all of which depend from independent claim 20, are also patentable over the combination of Hirano and Novak for reasons similar to those set forth above with respect to independent claim 20, and further in view of their own respective features.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection, and find claim 20 allowable over the applied references. Also, at least based on their respective dependencies to claim 20, claims 21-23 should be found allowable over the applied references, as well as for their respective additional distinguishing features.

Claims 32

Claim 32 is a dependent claim and necessarily includes all features of claim 31. As discussed above, Hirano fails to disclose all features of claim 31, and further Novak fails to cure the deficiencies of Hirano as noted above, with respect to claim 31. Novak does not teach what is missing from Hirano, for example the cipher module operates transparently as far as a user executing the application is concerned which is disclosed in claim 31. Therefore, claim 32 is patentable over Hirano and Novak taken alone or in combination for at lease the reasons provided above.

Claims 43-44

Claims 43-44 are dependent claims and necessarily include all features of claim 40. As discussed above, Hirano fails to disclose all features of claim 40, and further Novak fails to cure the deficiencies of Hirano as noted above with respect to claim 40. Novak does not teach what is missing from Hirano, for example the security information further including a file key and access rules wherein the security information is encrypted with a user key and can be decrypted with the user key when authenticated which is disclosed in claim 40. Therefore, claims 43-44 are patentable over Hirano and Novak taken alone or in combination for at lease the reasons provided above.

New Claims 51-56

New claims 51-56 are sought to be added. Claims 51-56 depend from independent claims 1, 11, 20, 24, 31, and 40, respectively, and should be found allowable for at least the reasons discussed above. Support for claims 51-56 can be found throughout the Specification, for example, figure 4C and paragraph 0097 of the instant application.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glenn J. Perry
Attorney for Applicants
Registration No. 28,458

Date: May 1, 2008

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

789868_2.DOC